IN THE UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Bridie Anne Wickstrom and
Jason Elmer Wickstrom,

Plaintiffs,

v.

City of Moose Lake; Carlton County; Pine County; Bridget Karp, acting in her individual capacity as an employee of the Carlton County Sheriff's Office; Randy Roberts, acting in his individual capacity as an employee of the Carlton County Sheriff's Office; John and Jane Does, acting in their individual capacities as supervisors, officers, deputies, staff, investigators, employees or agents of the Entity Defendants,

Defendants.

Case No. _____

COMPLAINT

JURY TRIAL DEMANDED

COMPLAINT

Plaintiffs Bridie Anne Wickstrom and Jason Elmer Wickstrom (collectively referred to as "Plaintiffs"), for their Complaint ("Complaint") against the above-named Defendants, hereby state and allege as follows:

General Background of Law and Facts

1. This is an action for injunctive relief and monetary damages for injuries sustained when Defendants City of Moose Lake, Carlton County, Pine County, Bridget Karp ("Karp"), Randy Roberts ("Roberts"), and John and Jane Does (collectively referred to as "Defendants") illegally obtained, disclosed, and/or used Plaintiffs' private, personal

and confidential drivers' license information without a legitimate or permissible law-enforcement purpose or any other lawful purpose, in violation of the Driver's Privacy Protection Act, 18 U.S.C. § 2721, *et seq*. ("DPPA"), also designated as private information under Minnesota law, Minn. Stat. § 171.12, subd. 7.

2. The City of Moose Lake, Carlton County, and Pine County ("Defendant Entities" or "Entity Defendants") employed Defendants Karp, Roberts, and John and Jane Does ("Defendant Individuals" or "Individual Defendants") as law-enforcement officers in their respective police and sheriff departments. Defendant Entities authorized Defendant Individuals, as part of their duties, to have access to the Minnesota Department of Public Safety's ("DPS") Driver and Vehicle Services Database ("DVS Database"), Bureau of Criminal Apprehension license plate database ("BCA Database"), and MyBCA Database ("MyBCA") (collectively, "State Databases"), all of which included license plate information and other private drivers' license information regarding Minnesota drivers.

3. Individual Defendants employed by Defendant Entities have viewed the private information of Plaintiff Bridie Wickstrom ("Bridie") at least 28 times since August 28, 2014 without a legitimate or permissible law-enforcement purpose or any other lawful purpose.

4. Attached to this Complaint as Exhibit A is a summary of accesses of Bridie's private driver's license information by personnel from the City of Moose Lake, Carlton County, and Pine County from January 13, 2012 to November 21, 2017. This summary is based on audits prepared by the Minnesota Department of Public Safety and

received by Bridie between November 14, 2014 and June 26, 2018. Although the summary includes lookups going back to 2012, Plaintiffs are only pursuing claims for impermissible accesses that occurred within the four years prior to the date of filing this Complaint.

5. Individual Defendants employed by Defendant Entities have viewed the private information of Plaintiff Jason Wickstrom ("Jason") at least 10 times since August 28, 2014 without a legitimate or permissible law-enforcement purpose or any other lawful purpose.

6. Attached to this Complaint as Exhibit B is a summary of accesses of Jason's private driver's license information by personnel from the City of Moose Lake, Carlton County, and Pine County from February 28, 2012 to March 8, 2018. This summary is based on audits prepared by the Minnesota Department of Public Safety and received by Jason between November 13, 2014 and June 26, 2018. Although the summary includes lookups going back to 2012, Plaintiffs are only pursuing claims for impermissible accesses that occurred within the four years prior to the date of filing this Complaint.

7. In September 2014, suspecting that their information may have been accessed impermissibly, Plaintiffs met with Sergeant Brian Belich at the Carlton County Sheriff's Office. Sergeant Belich told them he would call the BCA to check whether their information was being looked up. He later called Plaintiffs, informed them that no one had looked them up, and told them that they should "just drop it."

8. Prior to this date, effective August 1, 2014, Minnesota law, Minn. Stat. § 13.055, mandated that any government entity, whether a state agency or any political subdivision of the state, was required to disclose any breach of security of private or confidential data such as occurred here.

9. In approximately December 2014, Plaintiff Bridie Wickstrom contacted the BCA directly. Judy Strobel, Business Shared Services Manager, told her no one from Carlton County had ever called to obtain information regarding lookups of Bridie and Jason's information. This was in direct contravention to what Plaintiffs were told by Sergeant Brian Belich.

10. Bridie also spoke to BCA Director of Training and Auditing, Gary Link, who told her he had never seen so many lookups.

11. After Plaintiffs came to the Carlton County Sheriff's Office with their concerns, Defendant Carlton County knew or should have known Plaintiffs' information was being accessed. Nevertheless, Carlton County failed to take reasonable steps to investigate the potential impermissible accesses by its employees.

12. If Carlton County or any employee or official thereof did seek information concerning Plaintiffs' information being accessed as represented, then they failed to comply with their duties to notify the Plaintiffs of the unlawful accesses of their private information.

13. If Sergeant Brian Belich and Carlton County took no steps to identify whether there were inappropriate accesses of Plaintiffs' information as requested by

them, then they lied to Plaintiffs suggesting they had checked in a clear effort to persuade Plaintiffs not to pursue or discover the wrongdoing.

14. Plaintiffs have been harmed by Individual Defendants' unlawful obtainment, use, and/or disclosure of their private information and seek relief from this Court.

15. Congress enacted the DPPA in 1994 to prevent impermissible access, use, and disclosure of individuals' drivers' license information.

16. Congress restricted access, use, and disclosure of drivers' license information for only permissible purposes set forth in the statute.

JURISDICTION

17. This Court has subject matter jurisdiction over Count I pursuant to the DPPA, 18 U.S.C. § 2721, *et seq*. The aforementioned statutory and constitutional provisions confer original jurisdiction of this Court over this matter.

18. The DPPA claim in Count I is a federal claim arising under the above federal statute so that this Court is exercising federal question jurisdiction.

19. The amount in controversy exceeds $75,000, excluding interest and costs.

PARTIES

20. Plaintiff Bridie Wickstrom is, and was at all times material, a resident of the State of Minnesota and a citizen of the United States.

21. Plaintiff Jason Wickstrom is, and was at all times material, a resident of the State of Minnesota and a citizen of the United States.

22. Defendant City of Moose Lake is a city in Minnesota, which can be sued under Minn. Stat. § 466.01, *et seq*.

23. Defendant Carlton County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01, *et seq*.

24. Defendant Pine County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01, *et seq.*

25. Plaintiffs will refer to Defendants City of Moose Lake, Carlton County, and Pine County collectively as the "Defendant Entities" or "Entity Defendants."

26. Defendant Bridget Karp ("Karp") is, and was at all times material, a resident of the State of Minnesota, a citizen of the United States, and an employee of Carlton County.

27. Defendant Randy Roberts ("Roberts") is, and was at all times material, a resident of the State of Minnesota, a citizen of the United States, and an employee of Carlton County.

28. Defendants John and Jane Does, upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting in their individual capacities as law-enforcement supervisors, officers, or employees of the Defendant Entities or other federal, state, county, or municipal entities in Minnesota.

29. Plaintiffs will refer to the individual Defendants, including Karp, Roberts, and the John and Jane Does, collectively as the "Individual Defendants" or "Defendant Individuals."

FACTUAL ALLEGATIONS

The DVS and BCA Databases

30. The Driver and Vehicle Services Division of the DPS maintained motor vehicle records regarding each of the Plaintiffs.

31. The DVS Database contains "personal information" and "highly restricted personal information," as defined by 18 U.S.C. § 2725 ("Private Data"), including but not limited to names, dates of birth, drivers' license numbers, addresses, drivers' license photos, weights, heights, various health and disability information, and eye colors of Minnesota drivers, both current and former information dating back to the driver's first license issued in Minnesota.

32. The DVS Database may be accessed and queried by entering a person's name, license plate number, or driver's license number.

33. The BCA Database may be accessed and queried by different means, including by entering a person's name, license plate number, or driver's license number.

34. The DVS Database and the BCA Database contain Private Data.

Widespread Misuse of Private Data By Law Enforcement

35. In 2013, the Minnesota Legislative Auditor issued a report describing widespread misuse of the DVS Database by law enforcement in Minnesota. (Legislative Auditor's Report attached to this Complaint as Exhibit C).

36. In 2014, DVS terminated access of licensed law-enforcement officers to the DVS Database.

37. When access to the DVS Database changed for Minnesota's licensed law-enforcement officers, DVS provided access of motor vehicle records to licensed law-enforcement officers through a newly-created "MyBCA" portal.

38. Private Data is accessible through MyBCA and the related BCA Database.

39. Since 2014, DVS required law-enforcement personnel to obtain Private Data about Minnesota drivers through the MyBCA Database, although other individuals and entities who were previously permitted access to drivers' license data by DPS were still permitted to use the DVS Database.

40. Plaintiffs provided Private Data to DPS, including their addresses, color photographs, dates of birth, weights, heights, medical information, donor status, Social Security numbers, and eye colors for the purposes of acquiring and utilizing a Minnesota State driver's license.

41. The Private Data of Plaintiffs is protected from impermissible access, use, and disclosure by the DPPA and the MGDPA.

Plaintiffs

42. Plaintiff Bridie Wickstrom (f/k/a Bridie Dobosenski and Bridie Martin) has worked at Grand Casino Hinckley for approximately 23 years.

43. Plaintiff Jason Wickstrom is an inspector for the Avery and Enbridge pipelines, working mainly in the Milaca and Superior areas.

44. Bridie and Jason began dating in March 2014 and have lived together since approximately June 2014. They were married on September 30, 2017.

45. At the time Bridie and Jason began dating, both were in the process of divorcing their previous spouses. Jason's divorce from his ex-wife, Rhonda Wickstrom ("Rhonda") (n/k/a Rhonda Edwards) was particularly acrimonious.

46. In December 2014, Jason petitioned for and was granted an Order for Protection ("OFP") against Rhonda in Carlton County District Court.

47. On several occasions before the OFP was in place, the Carlton County Sheriff's Office was called to respond to disputes between Rhonda and Plaintiffs. On at least two occasions in 2015 and 2016, Plaintiffs called the Carlton County Sheriff's Office to report possible violations of the OFP by Rhonda. (To the extent that Carlton County Sheriff's Office accessed Plaintiffs' personal information in conjunction with these incidents, such accesses are not at issue in this case.)

Defendants' Misuse of Private Data

48. In 2014, Plaintiffs began to notice they were being pulled over frequently by law-enforcement officers, seemingly for no reason. The officers would tell them they had a taillight or license plate light out, but all lights were functioning properly when Plaintiffs checked.

49. On or about September 5, 2014, Plaintiffs went to the Carlton County Sheriff's Office to try to figure out why they were being stopped so often. They spoke to Sergeant Brian Belich, who said he would call the BCA to check whether their information was being looked up. Sergeant Belich later called Plaintiffs and told them no one had looked them up, that nothing unusual was going on, and that they should "just drop it."

50. Approximately one to two months after Plaintiffs discussed these concerns with Sergeant Belich, Jason received a phone call from Defendant Karp. In that conversation, Karp informed Jason that Rhonda had asked her to do different things for her, and Karp apologized to Jason for getting mixed up with Rhonda. The call was disconnected before Jason could ask Karp for more specifics about what she had done on Rhonda's behalf, and Karp did not answer the phone when Jason tried to call her back.

51. Plaintiffs later decided to follow up directly with the BCA. On or about December 8, 2014, Bridie spoke with Business Shared Services Manager, Judy Strobel, who told her there was no record of anyone from Carlton County contacting the BCA to check on lookups of Bridie and Jason's information.

52. Bridie also spoke to BCA Director of Training and Auditing Gary Link, who told her he had never seen so many lookups.

53. Upon information and belief, Rhonda is good friends with Defendant Karp.

54. Upon information and belief, Rhonda also has a personal relationship with Defendant Roberts.

55. Plaintiffs believe Rhonda used her connections to law-enforcement personnel to harass Plaintiffs and gain advantage over them in the divorce. Specifically, Plaintiffs believe Rhonda asked Karp to look up Plaintiffs' drivers' license and motor vehicle records as a way of investigating Plaintiffs' assets.

56. Plaintiffs believe Karp, Roberts, and other Individual Defendants also looked up Plaintiffs' information for purposes of satisfying their own curiosity regarding

individuals involved in a messy divorce that was a subject of gossip in their small community.

57. Under the DPPA, when Karp, Roberts, and John and Jane Doe employees of Entity Defendants made these unauthorized obtainments, Entity Defendants, which are themselves "persons" under the DPPA, also made these unauthorized obtainments.

58. Entity Defendants have lax policies and/or lax enforcement of these policies that allow for these intrusions.

59. Entity Defendants have inadequate practices of ascertaining and controlling the illegal access to individuals' private information by their employees.

60. Access to the Private Data was made by providing a user account and a password without reasonably requiring or ensuring that accesses would be limited to those for a legitimate purpose.

61. This form of disclosure was and is used not only for law-enforcement personnel but other recipients who have access to the DVS Database, including non-government employees, who comprise about half of the persons who have been granted access to the DVS Database.

62. Disclosures were made to law-enforcement personnel, including Individual Defendants, based simply upon the recipients' status.

63. Entity Defendants failed to reasonably ascertain or ensure that their Individual Defendant employees would use the State Databases permissibly.

64. Entity Defendants did not inquire from their Individual Defendant employees the purpose for which Plaintiffs' information was needed.

65. Entity Defendants failed to ascertain or ensure specifically that their Individual Defendant employees would use State Databases permissibly, that is, for a law-enforcement function.

66. Entity Defendants failed to provide reasonably adequate training in the permissible uses of the State Databases.

67. To the extent Entity Defendants delegated any part of their duties, they are still responsible for their Individual Defendant employees' obtainments and use of the State Databases.

68. Entity Defendants failed to monitor their Individual Defendant employees' activities on the State Databases, which they could have easily done by asking for audits from DPS.

69. In particular, Defendant Carlton County failed to request audits of its employees' lookups of Plaintiffs' private information even when Plaintiffs raised specific and reasonable concerns that their information may have been accessed improperly.

70. Defendant Carlton County lied about what it did do to address Plaintiffs' concerns and then presented inaccurate information to Plaintiffs.

71. Defendants' conduct creates an increased risk of identity theft for Plaintiffs.

72. Many viable methods were and are available to prevent the illegal obtainment of private information.

73. At all relevant times Entity Defendants had the ability to determine that drivers' license information was being accessed by their Individual Defendant employees.

74. Entity Defendants had the ability to prevent unauthorized access to the State Databases, including unauthorized access to Plaintiffs' Private Data.

75. Entity Defendants failed to prevent unauthorized access to the State Databases, including access to Plaintiffs' Private Data.

76. The policy of Entity Defendants is to uphold the provisions of the law, both state and federal, and to protect and safeguard the privacy rights of the State's citizens and inhabitants, including its drivers' privacy rights, and including those rights as are required to be protected by federal law.

77. Upon information and belief, it is the policy of Entity Defendants, as outlined in Minn. Stat. § 171.12, subd. 7, to comply with the provisions and requirements of the DPPA.

78. Entity Defendants and Individual Defendants all failed to follow Entity Defendants' policies.

79. Entity Defendants' failure exposed Plaintiffs' information to impermissible and knowing accesses by Individual Defendants.

80. Entity Defendants know that accesses to at least some of the State Databases could be made from personal computers.

81. Individual Defendants' and Entity Defendants' conduct in obtaining, disclosing, or using the Private Data for purposes not permitted under the DPPA was in willful and reckless disregard of federal law.

82. Individual Defendants' and Entity Defendants' obtainment and use of Plaintiffs' personal information was not for any use in carrying out any law-enforcement, governmental, judicial, or litigation-related function.

83. Individual Defendants' obtainment and use of Plaintiffs' personal information was for purposes that were purely personal to Individual Defendants.

84. Individual Defendants' purposes in obtaining information were personal and even malicious in nature.

85. Individual Defendants had no legitimate law-enforcement reason to obtain, disclose, or use Plaintiffs' personal information.

86. Individual Defendants were able to access the aforementioned Private Data by virtue of their agency relationships with Entity Defendants, and those relationships aided them in doing so.

87. Individual Defendants used Entity Defendants' computers and accessed the State Databases with passwords and credentials that were available to them because they were law-enforcement officers or otherwise employed by Entity Defendants.

88. Entity Defendants extended authority to Individual Defendants to use the State Databases and to access Plaintiffs' Private Data.

89. Individual Defendants had apparent authority from Entity Defendants to use the State Databases, unlike other employees of Entity Defendants who were not provided access.

90. The information in the State Databases was provided to Individual Defendants and other law-enforcement personnel of Entity Defendants for carrying out law-enforcement functions.

91. Entity Defendants provided State Database credentials for Individual Defendants' use in their roles as law-enforcement officers within the course and scope of their employment and Individual Defendants used those databases within the course and scope of their employment.

92. Each of the obtainments was committed knowingly; each of the obtainments was impermissible because Individual Defendants had no law-enforcement reason for accessing the information.

93. Individual Defendants obtained the information for personal reasons instead of law-enforcement reasons.

94. Individual Defendants viewed Plaintiffs' Private Data from their State-issued drivers' licenses including their home addresses, color photographs or images, dates of birth, eye colors, heights, weights, driver identification numbers, donor status, and medical information.

95. Individual Defendants made these accesses using Plaintiffs' names, drivers' license numbers, or license plates.

96. After Individual Defendants looked up Plaintiffs' Private Data, they gained knowledge of the contents of the Private Data. In gaining such knowledge, Individual Defendants obtained Plaintiffs' Private Data.

97. Individual Defendants knew that their obtaining of Private Data was unauthorized.

98. Individual Defendants obtained the Private Data of Plaintiffs for personal reasons, none of which reasons are permitted under the DPPA.

99. Without legitimate, permissible reasons, Individual Defendants obtained Plaintiffs' Private Data from the State Databases.

100. Upon information and belief, Individual Defendants further impermissibly used or disclosed Plaintiffs' Private Data.

101. These obtainments were committed surreptitiously, and without the knowledge of the victims (including Plaintiffs) when they occurred; the obtainments were kept hidden and concealed from the victims, including Plaintiffs.

102. Individual Defendants have never informed Plaintiffs that they accessed their information.

103. Individual Defendants went to great lengths to avoid letting Plaintiffs know they had accessed their personal private information.

104. The surreptitious, concealed, and hidden accesses are kept secret from the general public and from the victims, including Plaintiffs.

105. Plaintiffs bring this action for any illegal obtainments, disclosure, or use of Private Data by Defendants in the four years preceding the commencement of this lawsuit.

106. Whatever training, monitoring, or inquiry into the officers' usage of the information systems has been adopted is woefully inadequate to ensure that the databases are used properly and lawfully.

107. Despite any training undergone by Individual Defendants, Entity Defendants allowed them to obtain Plaintiffs' Private Data for unlawful purposes.

108. Upon information and belief, Entity Defendants permitted, condoned, or acquiesced in this illegal access to Plaintiffs' private information, and knew or should have known that it was occurring.

109. Upon information and belief, these illegal accesses occurred with regularity not only of Plaintiffs' private information, but of other Minnesota drivers' private information.

110. Entity Defendants either had no viable method or have an inadequate method of ascertaining and controlling the illegal access to individuals' private information by their officers.

111. The extent of this illegal access has been widespread and pervasive throughout departments, and has been a custom and practice.

112. The widespread practice is demonstrated by the systemic tolerance of illegal accesses.

113. Each user with access to the DVS Database has passwords allowing that individual access to that Database.

114. Entity Defendants' personnel can access the DVS Database from any computer with internet access.

115. Entity Defendants' personnel occasionally gave other individuals their passwords, contrary to requirements.

116. Each individual with access to the BCA Database has a password allowing that individual access to the BCA Database.

117. Each individual with access to the MyBCA Database has a password allowing that individual access to the MyBCA Database.

118. When Individual Defendants viewed Plaintiffs' private information, they did not do so to carry out official police functions.

119. It is unknown, at this time, how many times each Individual Defendant obtained, disclosed, or used Plaintiffs' Private Data.

120. Discovery can determine how many times each Individual Defendant did so.

121. Upon information and belief, Defendant Karp was one of the Individual Defendants who accessed Bridie's and Jason's information.

122. Upon information and belief, Defendant Roberts was one of the Individual Defendants who accessed Bridie's and Jason's information.

123. Based on the facts alleged above, each of the Plaintiffs had connections to law-enforcement personnel through Jason's ex-wife Rhonda.

124. Both Defendant Karp and Defendant Roberts work for the Carlton County Sheriff's Department.

125. The City of Moose Lake is located in Carlton County.

126. Pine County borders Carlton County.

127. Within the last four years, the Plaintiffs have lived in both Pine and Carlton Counties.

128. Plaintiffs are not pursuing claims for accesses they believe were related to legitimate traffic stops, calls for service, Orders for Protection, court proceedings, or other legitimate interactions they may have had with law-enforcement or other personnel of Defendant Entities.

129. At no time did Plaintiffs provide their express consent for Individual Defendants or Entity Defendants to obtain, disclose, or use their Private Data for any non-authorized purpose.

130. At no time did Plaintiffs behave in a manner that would provide any legal justification for Individual Defendants to invade their privacy.

131. Plaintiffs never waived the protections of the DPPA.

132. Defendants' actions have violated the DPPA.

133. Plaintiffs committed no crimes or transgressions that would explain or legitimize the unauthorized access of their Private Data by Defendants. Individual Defendants obtained Plaintiffs' personal information without probable cause or reasonable suspicion to believe that Plaintiffs had engaged in any criminal activity or any activity even remotely related to criminal activity at the times of the accesses at issue.

134. As a result of these invasions of privacy, Plaintiffs have suffered and continue to suffer emotional distress.

135. Defendants have damaged Plaintiffs' lives by these violations.

136. Plaintiffs are entitled to a determination that their rights have been violated, to an order enjoining further violations, and to monetary damages for these violations of federal law.

LEGAL CLAIMS

COUNT I – Violations of the Driver's Privacy Protection Act

18 U.S.C. § 2721, *et seq.*

(*Against Individual Defendants and Entity Defendants)*

137. Plaintiffs reaffirm and reallege the allegations in Paragraphs 1 through 136 as though fully set forth in this Paragraph 137.

138. Plaintiffs provided personal information to the DPS including their addresses, Social Security Numbers, color photographs, dates of birth, medical information, donor status, weights, heights, and eye colors for the purpose of acquiring and utilizing a State of Minnesota driver's license.

139. The State Databases also maintained Plaintiffs' driving records.

140. At no time did Plaintiffs provide their consent for Individual Defendants or Entity Defendants to obtain, disclose, or use Plaintiffs' Private Data for anything but official business.

141. Intentionally obtaining, disclosing, or using drivers' license information without an authorized purpose is a violation of the DPPA. The statute provides for criminal fines and civil penalties. 18 U.S.C. §§ 2723, 2724.

142. The DPPA creates an individual right to privacy in a person's driver's license information, thereby prohibiting unauthorized obtainment of all persons' information, including Plaintiffs'.

143. The DPPA provides redress for violations of a person's protected interest in the privacy of their motor vehicle records and the identifying information therein.

144. The Defendants, each of them, have invaded Plaintiffs' legally protected interest under the DPPA.

145. Individual Defendants and Entity Defendants knowingly obtained, and upon information and belief, knowingly disclosed or used Plaintiffs' Private Data from a motor vehicle record, for a purpose not permitted under the DPPA. 18 U.S.C. § 2724(a).

146. None of the Defendants' activities fell within the DPPA's permitted exceptions for procurement of Plaintiffs' private information.

147. Individual Defendants and Entity Defendants knew that Individual Defendants' actions related to the Plaintiffs' personal information were in violation of the DPPA.

148. Entity Defendants knew or should have known or recklessly disregarded that Individual Defendants were making these illegal accesses.

149. Entity Defendants knew that they did not ascertain what purpose Individual Defendants had in accessing the Private Data.

150. By the actions described above, Individual Defendants were acting within the course and scope of their employment when they obtained, disclosed, or used the Plaintiffs' Private Data from the State Databases for an impermissible purpose.

151. By the actions described above, Individual Defendants were acting with apparent authority when they obtained, disclosed, or used the Plaintiffs' Private Data from the State Databases for an impermissible purpose.

152. By the actions described above, Individual Defendants were aided-in-the-agency relationship when they obtained, disclosed, or used the Plaintiffs' Private Data from the State Databases for an impermissible purpose.

153. Individual Defendants used Entity Defendants' computers, passwords, and passcodes to obtain the Plaintiffs' Private Data.

154. Entity Defendants are vicariously liable for Individual Defendants' obtainments, disclosure, and use of Plaintiffs' Private Data for an impermissible purpose.

155. By the actions described above, Entity Defendants are directly liable as "persons" as defined by the DPPA for their obtainments, disclosure, and use of Plaintiffs' Private Data for an impermissible purpose.

156. Entity Defendants knowingly authorized, directed, ratified, approved, acquiesced in, committed, or participated in the obtainment, disclosure, or use of Plaintiffs' private personal information by Individual Defendants.

157. Entity Defendants are liable for the failure to train, monitor, and supervise Individual Defendants, who were improperly and unlawfully obtaining the private drivers' license information of citizens, including Plaintiffs, without a proper, lawful, permissible, or justifiable purpose for doing so.

158. In other lawsuits and potential lawsuits, DPS audits have revealed that officers in the Moose Lake Police Department and Pine County Sheriff's Office have made impermissible obtainments of the Databases.[1]

159. Upon information and belief, misuse of the State Databases has been well-known to municipalities like Entity Defendants. At a hearing at which DPS Commissioner Mona Dohman testified, the testimony of the Legislative Auditor revealed that at least 50% of law-enforcement officers are misusing the DVS Database by accessing, disclosing, and/or using the drivers' license personal information for an impermissible purpose.

160. The Legislative Auditor's Report showing such misuse is attached to this Complaint as Exhibit C.

161. Experts in the field of police training report that the primary complaint of many police departments is that law-enforcement personnel misuse private information. This is an established, well-known, and pervasive problem with law-enforcement that Entity Defendants have been unwilling to properly address.

162. Entity Defendants had the ability to determine if unauthorized access was being made and to prevent such unauthorized access to the State Databases, including of Plaintiffs' private information, through inquiries and requests for audits from DPS.

163. Entity Defendants failed to prevent unauthorized access to the State Databases, including of Plaintiffs' Private Data.

[1] See, e.g., *Engebretson v. Aitkin Cnty.*, Civil File No. 14-cv-01435 (ADM/FLN); *Heglund v. Aitkin Cnty.*, Civil File No. 14-cv-00296 (ADM/LIB); and *Kampschroer v. Anoka Cnty.*, Civil File No. 13-cv-02512 (SRN/TNL).

164. Plaintiffs have suffered harm because their private information has been obtained unlawfully. Plaintiffs suffered and continue to suffer harm by virtue of the increased risk that their protected information is in the possession of Individual Defendants, who obtained it without a legitimate purpose. This is precisely the harm Congress sought to prevent by enacting the DPPA and its statutory remedies.

165. As a direct and proximate result of Individual Defendants' and Entity Defendants' acts and omissions, Plaintiffs have been damaged in an amount yet to be determined, but believed to be well in excess of $75,000.00.

166. Plaintiffs are entitled to injunctive relief to prevent future impermissible obtainments, disclosures, and uses of their Private Data pursuant to 18 U.S.C. § 2724(b)(4).

167. The Defendants each willfully and recklessly disregarded the law, entitling Plaintiffs to punitive damages under the DPPA, see 18 U.S.C. § 2724(b)(2), which is not subject to the pleading requirement of Minnesota state law as set forth in Minn. Stat. § 549.20.

168. Plaintiffs are entitled to actual damages, punitive damages, reasonable attorneys' fees and other litigation costs reasonably incurred, and such other preliminary and equitable relief as the Court determines to be appropriate. 18 U.S.C. § 2724(b).

169. In addition, under the DPPA, Plaintiffs are each entitled to a baseline liquidated damages award of at least $2,500.00 for each violation of the DPPA. 18 U.S.C. § 2721(b)(1). Plaintiffs need not prove actual damages to receive said liquidated damages.

JURY DEMAND

170. Plaintiffs demand a trial by jury as to all issues of fact herein properly triable before a jury under any statutory or common law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment against the Defendants as follows:

1. Declare that the Defendants' conduct, as described in this Complaint, is unlawful;
2. A money judgment against all the Defendants for liquidated, actual, and compensatory damages in an amount in excess of Seventy-Five Thousand ($75,000.00) Dollars and punitive damages in an amount to be determined by the jury, together with their costs, including reasonable attorneys' fees, under the DPPA, and other applicable laws, and prejudgment interest;
3. Actual damages, punitive damages, attorneys' fees and other litigation costs, and such other preliminary and equitable relief as the Court determines to be appropriate under 18 U.S.C. § 2724(b);
4. Liquidated damages of at least $2,500.00 for each violation of the DPPA under 18 U.S.C. § 2721(b)(1);
5. Order Entity Defendants to adopt policies and practices designed to further deter and/or prevent Entity Defendants' personnel from unauthorized access to Plaintiffs' and other citizens' Private Data;

6. An injunction, permanently enjoining all Defendants from obtaining Plaintiffs' Private Data in violation of the DPPA, unless necessary for business-related or authorized purposes under the law;

7. For such other and further relief as this Court deems just and equitable.

SAPIENTIA LAW GROUP PLLC

Dated: August 28, 2018

s/Jonathan A. Strauss
Jonathan A. Strauss (#0279602)
Sonia Miller-Van Oort (#278087)
Lorenz F. Fett (#196769)
120 South Sixth Street, Suite 100
Minneapolis, MN 55402
Phone: (612) 756-7100
Fax: (612) 756-7101
jons@sapientialaw.com
soniamv@sapientialaw.com
larryf@sapientialaw.com

ATTORNEYS FOR PLAINTIFFS BRIDIE ANNE WICKSTROM AND JASON ELMER WICKSTROM